

**UNITED STATES DISTRICT COURT  
SOUTHERN DISTRICT OF OHIO  
WESTERN DIVISION**

**IN THE MATTER OF THE SEARCH OF  
INFORMATION THAT IS STORED AT  
PREMISES CONTROLLED BY GOOGLE  
ASSOCIATED WITH GOOGLE ACCOUNT ID:**

**CASE NO. 1:19-MJ-505**

**UNDER SEAL**

**GOOGLE ACCOUNT ID: 1037101965280  
E-MAIL: INTERSTATEFATZ@GMAIL.COM  
RECOVERY EMAIL:  
INTERSTATETHEGREAT@GMAIL.COM  
ALTERNATE EMAILS:  
INTERSTATEFATZ702@GMAIL.COM**

**AFFIDAVIT IN SUPPORT OF APPLICATION FOR  
SEARCH WARRANT**

I, Special Agent Brandon Burke, being first duly sworn, hereby depose and state as follows:

**INTRODUCTION AND AGENT BACKGROUND**

1. I am an investigative or law enforcement officer of the United States, within the meaning of Section 2510(7) of Title 18, United States Code, and am empowered by law to conduct investigations of, and to make arrests for, offenses enumerated in Section 2516 of Title 18, United States Code.

2. I am presently employed as a Special Agent (“SA”) of the Federal Bureau of Investigation (“FBI”), and have been so employed since December, 2007. I have experience conducting investigations into national and transnational criminal enterprises, organized crime, violent crimes, and criminal organizations that leverage technology during the course of their

crimes. I received instruction and training on, and have participated in, investigations involving possession with the intent to distribute and distribution of controlled substances, and conspiracies associated with the foregoing criminal offenses, which are prohibited by 21 U.S.C. §§ 841(a)(1), 846 (possession with intent to distribute narcotics and conspiracy to distribute narcotics), 843(b) (unlawful use of a communications facility to distribute controlled substances), and related narcotics-based financial crimes including violation(s) of 18 U.S.C. §§ 1956 (money laundering and conspiracy to commit money laundering) and 1957 (monetary transactions in criminally-derived property).

3. During the course of my law enforcement career, I have conducted and participated in the investigation of numerous criminal offenses, including those involved in the current investigation. I have experience investigating complex criminal enterprises with local, national, and transnational nexus. These investigations ranged from street gangs, outlaw motorcycle gangs, Mexican and South American criminal organizations, and criminal organizations that leverage cyber based techniques to further their criminal activity, such as drug trafficking and money laundering services. Through the course of conducting these investigations, I have been involved in the use of the following techniques: interviewing confidential human sources; conducting physical surveillance; conducting undercover drug operations in which drugs are purchased through the use of confidential human sources or undercover employees; consensual and court authorized monitoring and recording of telephonic communications; analyzing telephone pen registers and caller identification system data; analyzing data from mobile telephones; and executing search warrants and arrest warrants. I have also been involved in online and in-person undercover operations, as well as controlled drug deliveries and transactions.

4. In the course of my investigations and other cases on which I have worked, I have gained experience executing search warrants for physical premises, as well as for electronic evidence and data, including the content and other data associated with email, messenger, financial, and digital-marketplace accounts. I have become familiar with how criminal organizations, such money laundering organizations, use services provided by the email provider Google.<sup>1</sup> Furthermore, I am aware that Google stores and collects information from its users, including content from Gmail accounts, contacts list for cellular phones and emails, calendar entries, chat history, internet browsing history, location history, and how Google's Chrome OS platform that interacts with Chromebooks and allows living documents stored in Google Cloud services.

5. I am aware that criminal actors, such as money laundering organizations, will communicate via text message, phone calls, and internet applications, with their cellular telephone and other electronic devices prior to, during, and after the commission of a crime. This evidence is often uncovered during the forensic analysis of their cellular phone, electronic devices, and content obtained from email providers, internet service providers, and other technology providers, such as Google.

6. This affidavit is based upon: my personal knowledge; my review of documents and other evidence; my conversations with other law enforcement personnel and persons with subject matter expertise; and my training, experience and advice received concerning the use of computers in criminal activity and the forensic analysis of electronically stored information ("ESI"). Because this affidavit is being submitted for the limited purpose of establishing probable cause, it does not

---

<sup>1</sup> I am aware based on training and experience and prior legal process served to Google that Google provides services that include Android phone service, Gmail (email), calendar, Hangouts (chats), internet searching, location information, web and application activity, and YouTube, as well as other cellular and internet services.

include all the facts that I have learned during the course of my investigation. Where the contents of documents and the actions, statements, and conversations of others are reported herein, they are reported in substance and in part, except where otherwise indicated.

#### **PURPOSE OF THE AFFIDAVIT**

7. I make this affidavit in support of an application for a search warrant for information associated with a certain Google Account ID Administration (GAIA): **1037101965280**, and email address(es): **interstatefatz@gmail.com**, **interstatethegreat@gmail.com**, and **interstatefatz702@gmail.com** that is stored at premises owned, maintained, controlled, or operated by Google, and more particularly in Attachment A (the **Target Account**). This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Google to disclose to the government records and other information in its possession, pertaining to the subscriber or customer associated with the **Target Account**.

8. The purpose of this application is to seize property that constitutes evidence of the commission of a criminal offense, contraband, the fruits of crime and things otherwise criminally possessed designed or intended for use or which is or has been used as the means of committing a criminal offense as described herein, which constitute violations of law under:

- a. Title 18, U.S.C. § 1956 and 1957 - Money Laundering; and
- b. Title 21, U.S.C. § 846 and 841 – Conspiracy to Distribute a Controlled Substance.

9. This affidavit is based upon my own personal observations, my training and experience, discussions with other agents who are familiar with this investigation, and information collected during this investigation through, among other things, witness interviews, law

enforcement investigation reports, information obtained through searches, undercover operations, subpoena results, and public records.

### **FACTS ESTABLISHING PROBABLE CAUSE**

10. In 2018, the Southern Ohio Digitized Organized Crime Group (FBI, DEA, HSI, UPSIS, and local task force members) began working jointly with agencies in Las Vegas, Kansas City, and St. Louis to investigate the *Pill-Cosby & Slanggang* Dark Web Drug Trafficking Organization (DTO) (hereinafter referred to as “*PC-SG DTO*”), which operate from various dark web marketplaces.<sup>2</sup> The *PC-SG DTO* are poly drug vendor-based (‘vendor’ is a term synonymous with ‘drug trafficker’) organizations responsible for the distribution of controlled substances throughout the United States, including, *inter alia*, the Southern District of Ohio.

11. The investigation has revealed that the *Pill-Cosby* vendor-based DTO conspires with the *Slanggang* DTO to distribute controlled narcotics, to include fentanyl, a scheduled II controlled substance. The *PC-SG DTO* base their operation from Las Vegas, Nevada to manufacture, package, and distribute drugs through the U.S. mail system and around the country to its customers. The *PC-SG DTO* vender profiles on dark web markets offer for sale (listings) “pressed oxy,” which investigators know to contain fentanyl. The *PC-SG DTO* negotiates drug purchases on these marketplaces in exchange for virtual currency, namely bitcoin (BTC).<sup>3</sup>

---

<sup>2</sup> The “dark web” is a portion of the Deep Web of the Internet, where individuals must use an anonymizing software or application called a “darknet” to access content and websites. Within the dark web, criminal marketplaces operate, allowing individuals to buy and sell illegal items, such as drugs, firearms, and other hazardous materials, with greater anonymity than is possible on the traditional Internet (sometimes called the “clear web” or simply the “web”). These online market websites use a variety of technologies, including the Tor network (defined below) and other encryption technologies, to ensure that communications and transactions are shielded from interception and monitoring. Famous dark web marketplaces, also called Hidden Services, such as Silk Road, AlphaBay, and Hansa (all of which have since been shut down by law enforcement), operated similarly to clear web commercial websites such as Amazon and eBay, but offered illicit goods and services.

<sup>3</sup> Since Bitcoin is both a cryptocurrency and a protocol, capitalization differs. Accepted practice is to use “Bitcoin” (singular with an uppercase letter B) to label the protocol, software, and community, and “bitcoin” (with a lowercase letter b) to label units of the cryptocurrency. That practice is adopted here.

*Slanggang* also offers their drug distribution services via the Wickr platform, a well-known mobile instant messenger application that employs end-to-end encrypted and content messages that expire after a pre-set time. Based upon the ensuing information, and the totality of the investigation, investigators believe Sean DEAVER, a Las Vegas resident, primarily operates the *Pill-Cosby* vendor moniker.

#### Undercover Drug Purchases

12. During the course of the investigation, numerous online undercover drug purchases have been made from the monikers, *Pill-Cosby* and *Slanggang*, many among which were delivered to the Southern District of Ohio. In several of these purchases, undercover agents placed an order for drugs, such as “pressed oxy,” in exchange for bitcoin.

13. On June 25, 2018, an undercover purchase of “50x pressed oxy 30mg” was made from *Pill-Cosby* for 0.71 BTC (\$446.00) on the Dream marketplace. A laboratory examination of the drug evidence was conducted by the Hamilton County Ohio Crime Laboratory, which revealed the presence of fentanyl. On April 17, 2019, an undercover purchase of crystal methamphetamine was made from *Pill-Cosby* on the Empire marketplace for 0.18173 BTC (\$955.00). Ten pressed fentanyl pills were added as a bonus to the order. On May 7, 2019, an undercover purchase of pressed fentanyl was made from *Slanggang* on Wickr, using Wickr ID: *Slanggangrick*, for 0.13300 BTC (\$780.00). All “pressed oxy” and “pressed fentanyl” purchases made thus far from *Pill-Cosby* and *Slanggang* were found to contain pills packaged in a similar fashion and to also contain pills of similar shape, color, size, and bearing the pill imprint “A 215” and a half tablet score. A laboratory examination for both items of drug evidence was conducted by the Hamilton County Ohio Crime Laboratory, which revealed the presence of fentanyl in the pressed pills sent by both vendors.

Financial Investigation

14. Regarding the June 25, 2018, undercover drug purchase, a review of USPS databases indicates that this parcel was purchased by an EasyPost postage meter. According to the USPS, there were several BTC transactions associated with the *Pill-Cosby* shipping label. Based upon this data, a federal Grand Jury subpoena was issued to Coinbase, a digital (virtual) currency exchange located in the United States. Coinbase revealed the following customer accounts to be associated with one another: Sean DEEVER (Coinbase account number: 59d1d5c0269d7a011a63e953), Abby JONES (Coinbase account number: 5892c25653fc49007f232447), and Demetra ISBELL (Coinbase account number: 563c0f0d9ac69f0880000032). The investigation has revealed Abby JONES is in a relationship with Sean DEEVER and that they reside with one another, while Demetra ISBELL is the mother to Khlari SIROTKIN, another subject in this investigation, all as outlined below.

15. Based upon the foregoing, Cincinnati-based investigators discovered that DEEVER has a criminal history involving drug distribution. Through a review of open source social media, DEEVER promoted himself as a rapper by the name of “*interstatefatz*.” According to the Coinbase return for DEEVER, he supplied his email as, interstatefatz@gmail.com (**Target Account**). Further, DEEVER is connected to Khlari SIROTKIN and SIROTKIN’s girlfriend/associate, Kelly STEPHENS, through social media.

Google Search Warrant Return in Cause # 1:19MJ-326

16. The investigative team believes Khlari SIROTKIN and his girlfriend/associate, Kelly STEPHENS, operate the *Slanggang* moniker. On or about May 2019, Google responded to the execution of a federal search warrant (cause #: 1:19MJ-326) on several Gmail accounts associated with SIROTKIN and STEPHENS. According to Google’s response, email

communications between SIROTKIN and STEPHENS revealed a conspiracy between them to traffic drugs via dark web markets. For example, on February 24, 2019, SIROTKIN, using email account: cryptoklizo@gmail.com, emailed STEPHENS, using, kellycomatose@gmail.com, “...don’t worry about work (selling drugs online) they (the marketplace administrators) still haven’t even approved our profile for vending (marketplace vendor profile link).” The next day SIROTKIN emailed STEPHENS, “I just checked and they (marketplace administrators) approved fatz (DEAVER) new vendor profile today.” As demonstrated, the Google response revealed “fatz” (aka *interstatefatz*, which is DEAVER) operates another vendor site, believed to be *Pill-Cosby* profile.

17. Also discovered in the aforementioned Google return were photographs (contained in STEPHENS’ account) of a pill-press (photograph below), which investigators believe is used to manufacture the pressed fentanyl pills, purchased by undercover investigators. Further, there is documentation in the Google return that indicates pill-press parts were purchased by SIROTKIN.





Google Records for the **Target Account**

18. On November 7, 2018, Google responded to a federal Grand Jury subpoena for accounts associated with “interstatefatz@gmail.com,” which identified the **Target Account** subscriber account data contained in this affidavit for DEEVER. According to Google’s response, DEEVER accessed his **Target Account** on June 24, 2018, from IP address: 76.164.224.214. Records received from Binance (an international cryptocurrency exchange) indicated that in November 2017 the IP address was used to access the Binance account belonging to SIROTKIN, which further substantiates the illicit connection between SIROTKIN and DEEVER.

**BACKGROUND CONCERNING GOOGLE ACCOUNTS**

19. In my training and experience, I have learned that Google Inc., provides a variety of on-line services, including electronic mail (“email”) access, to the public. Google Inc., allows subscribers to obtain email accounts at the domain name, gmail.com, such as the email accounts listed in Attachment A. Subscribers obtain an account by registering with Google Inc. During the registration process, Google Inc., asks subscribers to provide basic personal information. Therefore, the computers of Google Inc., are likely to contain stored electronic communications (including retrieved and unretrieved email for Google Inc., subscribers) and information concerning subscribers and their use of Google Inc., services, such as account access information, email transaction information, and account application information. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account’s user or users.

20. Furthermore, the computers of Google are likely to contain stored electronic communications (including retrieved and un-retrieved email for Google users and information

concerning subscribers and their use of Google services, such as account access information, email transaction information, and account application information). In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

21. Google provides services called Google Drive and Google Keep. Google Drive allows users to create, store, edit, and share files, including, through a suite of productivity apps (Docs, Sheets, and Slides) documents, spreadsheets, and presentations. Google Drive may also contain data used by third-party apps, such as WhatsApp backup files. Google Keep allows users to quickly create, update, and share notes and lists. Users can also add images to notes and lists created with Google Keep. Files on Google Drive, and notes and lists on Google Keep, remain on Google servers indefinitely unless deleted by the user, and for a period of time following deletion. In my training and experience, evidence of who was using a Google account and evidence related to criminal activity of the kind described above, may be found in these files and records.

22. A Google subscriber can also store with the provider files in addition to emails, such as address books, contact or buddy lists, calendar data, pictures (other than ones attached to emails), and other files, on servers maintained and/or owned by Google. As noted above, the Google account and Gmail address(es) listed in Attachment A also uses additional Google services to include; Android, Gmail, Google Calendar, Google Hangouts, Google+, Has Google Profile, Has Plusone, Location History, Minutemaid, Web & App activity, and YouTube. In my training and experience, I am aware that Google stores a user's information on their servers for some of these services, such as Google Hangouts, Location History, and Web & App activity. These services may constitute evidence of the crimes under investigation. Google Hangouts is a unified communications service that enables text, voice, or video chats, either one-on-one or in a group.

Google Location Services collects data to improve location-based services. For example, a user can get web search results and ads based on their device's location. Web & App activity contain internet browsing history and other Google app history.

23. In my training and experience, email providers generally ask their subscribers to provide certain personal identifying information when registering for an email account. Such information can include the subscriber's full name, physical address, telephone numbers and other identifiers, alternative email addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number). In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users. Based on my training and my experience, I know that, even if subscribers insert false information to conceal their identity, this information often provides clues to their identity, location, or illicit activities.

24. In my training and experience, email providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (*i.e.*, session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via the provider's website), and other log files that reflect usage of the account. In addition, email providers often have records of the Internet Protocol address ("IP address") used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the email account.

25. In my training and experience, in some cases, email account users will communicate directly with an email service provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. Email providers typically retain records about such communications, including records of contacts between the user and the provider's support services, as well as records of any actions taken by the provider or user as a result of the communications. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

26. As explained herein, information stored in connection with an email account may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, the information stored in connection with an email account can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, email communications, contacts lists, and images sent (and the data associated with the foregoing, such as date and time) may indicate who used or controlled the account at a relevant time. Further, information maintained by the email provider can show how and when the account was accessed or used. For example, as described below, email providers typically log the Internet Protocol (IP) addresses from which users access the email account, along with the time and date of that access. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the email account access and use relating to the crime under investigation. This geographic and timeline information may tend to either inculcate or

exculpate the account owner. Additionally, information stored at the user's account may further indicate the geographic location of the account user at a particular time (*e.g.*, location information integrated into an image or video sent via email). Last, stored electronic data may provide relevant insight into the email account owner's state of mind as it relates to the offense under investigation. For example, information in the email account may indicate the owner's motive and intent to commit a crime (*e.g.*, communications relating to the crime), or consciousness of guilt (*e.g.*, deleting communications in an effort to conceal them from law enforcement).

27. Based on the foregoing facts asserted and on my experience with the persistence of information maintained within such accounts, I believe it likely that evidence of the sort described in this Affidavit and Attachments remains within the **Target Account** even today.

#### **INFORMATION TO BE SEARCHED AND THINGS TO BE SEARCHED**

28. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular, 18 U.S.C. §§ 2703(a), and 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrant to require Google to disclose to the government copies of the records and other information (including the content of communications) particularly described in Section I of Attachment B. Upon receipts of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

#### **CONCLUSION**

29. Based on my training and experience, and the facts as set forth in this affidavit, there is probable cause to believe that there exists evidence, instrumentalities, contraband and/or fruits of the crimes described above on premises controlled by the Provider, Google. Accordingly, a search warrant is requested. Because the warrant will be served on Google who will then compile

the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

### **RETENTION OF INFORMATION FOR AUTHENTICATION**

30. In anticipation of litigation relating to the authenticity of data seized pursuant to the warrant, the Government request that it be allowed to retain a digital copy of all seized evidence authorized by the Warrant for as long as is necessary for authentication purposes.

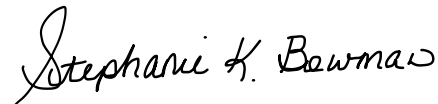
### **SEALING REQUEST**

31. It is respectfully requested that the Court issue an order sealing, until further order of the Court, all papers submitted in support of the requested search and seizure warrant(s), including the application(s), this affidavit, the attachments, and the requested search warrant. I believe that sealing these documents is necessary because the information to be seized is relevant to an ongoing investigation and includes references to cooperating individuals. Premature disclosure of the contents of the application, this affidavit, the attachments, and the requested search warrant may adversely affect the integrity of the investigation, including giving targets a chance to destroy evidence or take other steps to hinder the investigation.



SPECIAL AGENT BRANDON BURKE  
Federal Bureau of Investigation

Sworn to before me on  
July 10, 2019,



HON. STEPHANIE K. BOWMAN  
UNITED STATES MAGISTRATE JUDGE  
SOUTHERN DISTRICT OF OHIO

**ATTACHMENT A**

This warrant applies to information associated with Google Account ID Administration (GAIA): **1037101965280**, and email address(es): **interstatefatz@gmail.com**, **interstatethegreat@gmail.com**, and **interstatefatz702@gmail.com**, that is stored at premises owned, maintained, controlled, or operated by Google LLC, a company headquartered at 1600 Amphitheatre Parkway, Mountain View, California 94043.

**ATTACHMENT B**

**Particular Things to be Seized**

**I. Information to be disclosed by Google Inc. (the “Provider”)**

To the extent that the information described in Attachment A is within the possession, custody, or control of the Provider, regardless of whether such information is located within or outside of the United States, and including any emails, records, files, logs, or information that has been deleted but is still available to the Provider occurring after January 1, 2018, the Provider is required to disclose the following information to the government for each account or identifier listed in Attachment A:

a. The contents of all emails associated with the account, including stored or preserved copies of files and emails sent to and from the account, draft emails, the source and destination addresses associated with each email, the date and time at which each email was sent, and the size and length of each email;

b. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative email addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);

c. The types of service utilized;

d. All records or other information stored by an individual using the account, including address books, contact and buddy lists, calendar data, pictures, and files; and

e. All records and information for the following services, but not limited to only these services, if other exists:



- i. Android
- ii. Contacts
- iii. Gmail
- iv. Google AdSense
- v. Google Alerts
- vi. Google Analytics
- vii. Google Calendar
- viii. Google Docs
- ix. Google Drive
- x. Google Hangouts
- xi. Google My Maps
- xii. Google Payments
- xiii. Google Photos
- xiv. Google+
- xv. Has Google Profile
- xvi. Has Plusone
- xvii. Knowledge Search
- xviii. Web & Activity
- xix. YouTube
- xx. iGoogle

- f. All location information obtained for the user's account through Google's Location History;
- g. All internet browsing history for the user's account; and

h. All records pertaining to communications between the Provider and any person regarding the account, including contacts with support services and records of actions taken.

**II. Information to be seized by the government**

All information described above in Section I that constitutes evidence of violations of 21 U.S.C. §§ 841(a)(1), 846 (possession with intent to distribute narcotics and conspiracy to distribute narcotics), 843(b) (unlawful use of a communications facility to distribute controlled substances), and related narcotics-based financial crimes including violation(s) of 18 U.S.C. §§ 1956 (money laundering and conspiracy to commit money laundering) and 1957 (monetary transactions in criminally-derived property), occurring after January 1, 2018, including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

- a. Information regarding the acquisition, purchase, sale, or transfer of controlled substances or the proceeds therefrom.
- b. Evidence indicated how and when the account was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crime under investigation and to the account owner;
- c. Evidence indicating the account owner's state of mind as it relates to the crime under investigation;
- d. The identity of the person(s) who created or used the user ID, including records that help reveal the whereabouts of such person(s).

The Provider is hereby ordered to disclose the above information to the government within **14 days** of service of this warrant.